Federal Public Key Infrastructure Policy Authority (FPKIPA)
Minutes of the 12 April 2005 Meeting
GSA; 1800 F Street; Room G225; Washington, DC

A.   AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discuss/Vote on Minutes from 8 March 2005
3) Status of Email Votes Since Last FPKIPA Meeting
4) Topic #1: Update on US Citizenship Issue for FBCA CP
5) Topic #2: Status of Compliance Audit Frequency Point Paper
6) Federal Identity Credentialing Committee (FICC) Report
7) FPKI Certificate Policy Working Group (CPWG) Report
8) Federal PKI Operational Authority (FPKI OA) Report
9) Final Meeting Items – Other topics, Action Items, Proposed agenda items for next meeting
10) Meeting Adjourned

B.   ATTENDANCE LIST

VOTING MEMBERS

Organization	Name	Email	Telephone
Dept of Commerce (NIST)	Polk, Tim		
Dept of Defense	Hanko, Dave		
Dept of Energy	Breland, Mary Ann		
Dept of Health & Human Services	Alterman, Peter		
Dept of Homeland Security	Hagerling, Don		
Dept of Justice	Morrison, Scott		
Dept of State	Cao, Tin		
Dept of the Treasury	ABSENT		
GSA	Temoshok, David		
NASA	ABSENT		
OMB	ABSENT		
USDA/NFC	Sharp, Kathy		
USPTO	Purcell, Art		

OBSERVERS

Organization	Name	Email	Telephone
Dept of Defense	Mitchell, Debbie		
Dept of Homeland Security	Shomo, Larry		
Dept of Justice	Hornung-Kobes, Lynette		
FICC	Spencer, Judy		
FICC Support	Petrick, Brant		
FPKI OA Director (GSA)	Jenkins, Cheryl		
FPKI OA (Mitretek)	Tate, Darron		
FPKIPA Secretary (Booz Allen Hamilton)	Lentz, Mark		
State of Illinois	Anderson, Mark		
Treasury (eValid8)	Dilley, Brian		

C.   MEETING ACTIVITY

Agenda Items 1 & 2

Introductions / Vote on Approval of Meeting Minutes
This meeting took place at the GSA Headquarters Building, 1800 F Street, Washington, DC in Room G225. Dr. Peter Alterman, Department of Health & Human Services (HHS) and FPKIPA Chair, called the meeting to order at 9:45 a.m. with attendee introductions.

The 08 March 2005 meeting minutes were recommended by motion for approval vote (GSA) and seconded (Commerce). These minutes were unanimously approved by voice vote.

Agenda Item 3

Status of Email Votes Since Last FPKIPA Meeting
There were two items voted on via email votes since the last FPKIPA meeting on 8 March 2005. The email vote records for these items are attached as Appendix A of these minutes.

Mr. Mark Lentz, Booz Allen Hamilton and the FPKIPA Secretary, provided a brief summary of the outcome of the email vote for each of the two items:

DHS Technical Testing – The DHS Technical Testing was explained at the 8 March FPKIPA meeting but the test report needed to be revised based on comments made at that meeting, so an email vote was requested once the report was revised. The email vote request was requested on 9 March and due on 11 March. 7 voting members voted Yes (58%), 1 voting member voted No (8%), 1 voting member voted Abstain (8%), and 3 voting members did not cast their vote (25%). Therefore, the DHS Technical Testing was approved.

DHS Cross-Certification (Medium) -10 voting members voted Yes (83%) and 2 voting members did not cast their votes (17%) to approve DHS for cross-certification at the Medium assurance level. As a result of this vote, this is the first FPKIPA meeting attended by DHS as a voting member.

Agenda Item 4

Topic #1: Update on US Citizenship issue for FBCA CP
Since the 24 February 2005 meeting on this issue, Ms. Judith Spencer has been leading the effort to develop a solution that provides a more accurate, quantifiable, realistic, and feasible metric for trustworthy, loyal, and integrity - regardless of national origin or citizenship of the PKI authorities.

The DoD believes this is a very important issue and that maintaining the U.S. citizenship portion of the requirement in the FBCA CP, Section 5.3.1 is critical as part of any solution. DoD is concerned that removing U.S. citizenship from the requirement waters down this requirement.

As part of developing a revised requirement and better solution on this subject, Ms. Spencer has asked the Legal and Policy Working Group (LPWG) to review and comment on this issue from a legal perspective. The LPWG and the ad-hoc US Citizenship working group, led by Ms. Spencer after the 24 February meeting, are working on a position paper on this subject.

DHS also agrees with the importance of this issue but identified the PKI authority's trustworthiness as the most important aspect of this requirement. They mentioned the clearance process as being a good mechanism to provide the appropriate metrics for trustworthiness. One option to address the use of

non-US citizens in PKI authority roles would be to audit or supervise the actions of the non-US citizen in such a way that they must have critical actions reviewed by a US citizen member or manager of the CA staff. Another option would be to still require US citizenship for all PKI authority roles, but have a robust waiver process for addressing the use of non-US citizens.

To make significant progress on a resolution to this issue, it appears that another US Citizenship meeting (government only this time) should be held to allow more dialogue on the issue and to work out a meaningful solution. The 2nd week of May will be the target meeting time frame.

ACTION (130): Mr. Tim Polk, Department of Commerce (NIST) will propose two dates during the 2nd week of May 2005 to choose from for scheduling a meeting for government only FPKIPA members to discuss concerns and facilitate development of solution options for the US citizenship issue.

Agenda Item 5

Topic #2: Status of Compliance Audit Frequency Point Paper
On 11 April 2005, a meeting was held between Ms. Kathy Sharp, USDA/NFC; Ms. Cheryl Jenkins, GSA and the FPKIA OA Program Manager; Dr. Peter Alterman, HHS and FPKIPA Chair; and Mr. Mark Lentz, Booz Allen Hamilton and FPKIPA Secretary. The subject of that meeting was discussion of the current dilemma for the FBCA Cross-Certification members in complying with the FBCA CP requirement for a yearly compliance audit.

Ms. Sharp led the discussion in this FPKIPA meeting. She said that one solution to not doing a formal full audit each year would be to have the organization do a self-assessment of their operations and if there have been no significant changes in the past year, then an audit is not necessary. The voting members in attendance did not agree that a self-assessment would be a suitable process.

After some discussion about how audits are conducted and what would be feasible, the group generally agreed that an independent auditor is probably necessary to do some type of audit each year, but that after the 1st year full audit, it may be possible to arrange for the 2nd and 3rd year audits to be specifically contracted with the auditor to have a reduced scope and then the 4th year audit would be a full audit again.

ACTION (131): Ms. Cheryl Jenkins, GSA and FPKIA OA Program Manager, and DoD will work together on a draft position paper on this issue and report to the FPKIPA at the 14 June FPKIPA meeting.

On a related topic, the State of Illinois notified the FPKIPA Chair since the 8 March FPKIPA meeting that they needed an extension on the period for their annual compliance audit due to difficulty in finding a qualified and available auditor. The DoD motioned that the FPKIPA vote to approve for the State of Illinois an extension for their compliance audit until 30 June 2005. The motion was seconded by DHS and approved unanimously per the following voting record:

Approval vote for extension of State of Illinois Compliance Audit until 30 June 2005			
Voting members	Vote (Motion – DoD; 2nd – DHS)		
	Yes	No	Abstain
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Health & Human Services	X		
Dept of Homeland Security	X		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury (designated proxy – FPKIPA Chair)	X		
GSA	X		
NASA	ABSENT – did not vote		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Agenda Item 6

Federal Identity Credentialing Committee (FICC) Report
The FICC Handbook comment period has closed, but agencies can still provide comments.

NIST Special Publication 800-73, the technical specification for Smart Cards, has been finalized.

NIST Special Publication 800-78, Recommendation for Cryptographic Algorithms and Key Sizes, has been distributed for comment.

NIST Special Publication 800-76, the technical specification for Biometrics (defining fingerprint specifications only) has also been distributed for comment.

The Smart Card IAB met and has a position on Smart Card acquisition moving forward and comments will be due by the end of April.

Agenda Item 7

FPKI Certificate Policy Working Group (CPWG) Report
Mr. Tim Polk, Department of Commerce (NIST) and CPWG Co-Chair, led the CPWG Report.

Department of Justice Policy Mapping
The CPWG reviewed the Department of Justice policy mapping for the High assurance level initially at the 1 March CPWG meeting. There were only six areas of discrepancy after reviewing both the General and High assurance mapping matrices. The Department of Justice responded to the CPWG comments with their revised CP, version 1.09, dated 18 March 2005. The CPWG determined that the areas of discrepancy were successfully addressed by the CP revisions. Therefore, the CPWG recommended the Department of Justice policy mapping at the High assurance level for FPKIPA approval.

The following table shows the voting record for the Department of Justice policy mapping:

Approval vote for Department of Justice policy mapping (High)			
Voting members	Vote (Motion – Commerce; 2nd – State)		
	Yes	No	Abstain
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Health & Human Services	X		
Dept of Homeland Security			X
Dept of Justice	Cannot vote --- Conflict of Interest		
Dept of State	X		
Dept of the Treasury (designated proxy – FPKIPA Chair)	X		
GSA	X		
NASA	ABSENT – did not vote		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Department of Homeland Security Policy Mapping and Cross-Certification (Basic & High)
The CPWG reviewed the Department of Homeland Security (DHS) policy mapping for the Basic and High assurance levels initially at the 23 March CPWG meeting. The General and Medium policy mapping had already been previously FPKIPA approved via email on 11 March 2005. There were only four areas of discrepancy after reviewing both the Basic and High assurance mapping matrices. The DHS responded to the CPWG comments with their revised CP, version 2.3 dated 6 April 2005. The CPWG determined that the areas of discrepancy were successfully addressed by the CP revisions. Therefore, the CPWG recommended the Department of Homeland Security policy mapping at the Basic and High assurance level for FPKIPA approval.

The following table shows the voting record for the DHS policy mapping (Basic & High):

Approval vote for Department of Homeland Security policy mapping (Basic & High)			
Voting members	Vote (Motion – Commerce; 2nd – PTO)		
	Yes	No	Abstain
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Health & Human Services	X		
Dept of Homeland Security	Cannot vote --- Conflict of Interest		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury (designated proxy – FPKIPA Chair)	X		
GSA	X		
NASA	ABSENT – did not vote		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Because the FPKIPA had just recently approved DHS for cross-certification at the Medium assurance level on 18 March, and DHS had already fulfilled the technical testing and compliance audit

requirements, DHS was ready for approval vote for cross-certification at the Basic and High assurance levels.

The following table shows the voting record for the DHS Cross-Certification (Basic & High):

Approval vote for Department of Homeland Security Cross-Certification (Basic & High)			
Voting members	Vote (Motion – Commerce; 2nd – DoD)		
	Yes	No	Abstain
Dept of Commerce	X		
Dept of Defense	X		
Dept of Energy	X		
Dept of Health & Human Services	X		
Dept of Homeland Security	Cannot vote --- Conflict of Interest		
Dept of Justice	X		
Dept of State	X		
Dept of the Treasury (designated proxy – FPKIPA Chair)	X		
GSA	X		
NASA	ABSENT – did not vote		
OMB	ABSENT – did not vote		
USDA/NFC	X		
USPTO	X		

Status of FBCA CP (RFC 3647)

Mr. Polk explained the process at the recent CPWG meetings held on 5&6 April to review the FBCA CP analysis conducted by KPMG. The overall result of the KPMG analysis was that there were no new requirements in the RFC 3647 version of the FBCA CP that would require a special audit of the FPKIA OA, which means that the FBCA CP (RFC 3647) can be recommended for FPKIPA approval shortly after the next CPWG meeting on 27 April, when some final outstanding comments are resolved.

Next CPWG meeting

1) 27 April – regular CPWG meeting @ Booz Allen Hamilton, National Business Park facility

Agenda Item 8

Federal PKI Operational Authority (FPKI OA) Report

Status of CP/CPS Compliance Audit:

Ms. Cheryl Jenkins, FPKI OA Director, reviewed the status of the FPKIA CP/CPS Compliance Audit, stating the following highlights:

KPMG finished the FPKIA CP/CPS audit and the report will be sent to the FPKIPA mail list.

The RFC 2527 vs. RFC 3647 FBCA CP analysis was completed by KPMG by 31 March 2005 and reviewed by the CPWG during their 2-day working session on 5-6 April 2005, as reported during the CPWG report.

Technical Updates:
Certificate Validation
Some updates have been made to CAM. Testing with the updated CAM has produced mixed results – testing in the open LDAP environment has been fine but testing in the production environment has surfaced some technical issues. Testing is continuing to work out the technical issues.

Testing Environment
The FPKI OA stressed again the importance of each FBCA cross-certification member establishing and maintaining a test CA and architecture that mirrors the configuration and capability of their production system. Having this test capability at each FBCA cross-certification member organization will greatly assist in the resolution of the current certificate validation technical issues and all future technical issues. In fact, having the test capability would also facilitate proactive Bridge-To-Bridge (B2B) and directory testing across multiple bridges.

Certificate Validation RFI
This RFI has been released and a large, more than expected response has been received to date.

Status of FBCA/Applicant Cross-Certification Technical Testing:
Government Printing Office (GPO) - technical testing was completed on 31 March and the report will be completed in time for voting at the 10 May FPKIPA meeting.

Wells Fargo – Testing with Wells Fargo hasn't started yet, as they are currently deciding on a public directory product.

Boeing – Testing hasn't started yet.

Department of Justice – Testing hasn't started yet.

Status of CA Testing:
There was no CA testing since the 8 March FPKIPA meeting to report during this meeting.

Agenda Item 9

Final Meeting Items

DHS Request for Common Policy CA Certificate in the Vendors' Root Cert Cache
DHS asked if there should be a FPKI strategy for issuing signed email messages of national importance from an organization (e.g. DHS, DoD, Dept of State, Dept of the Treasury, etc) that could be handled by Subscribers that are outside the FBCA community. After some brief discussion on possible solutions, the best solution would probably be to post the Common Policy CA certificate in the certificate root store cache of the leading email vendor products. This would be easier than posting each agency's CA certificate and most citizens trust root certificates in the root store cache of commercial products. Department of the Treasury and the State Department have also initiated the certificate root store with commercial vendors for the same reasons.

ACTION (132): The FBCA TWG will be tasked with determining the Level Of Effort (LOE) and cost necessary to post the Common Policy CA certificate in the root store cache of leading email vendor products and report their findings at a future FPKIPA meeting.

Treasury PKI Architectural Changes
The Department of the Treasury announced that it will soon send a letter to the FPKIPA Chair informing the FPKIPA of Treasury PKI architectural changes.

Next FPKIPA Meeting
The next FPKIPA Meeting is scheduled for 10 May 2005 from 09:30-12:30 at the GSA facility located at 1800 F Street, Room 5141A, Washington, DC. The proposed unique topics for this meeting will be an update on the status of both the FBCA CP (RFC 3647) and the FPKIPA By-Laws document.

<div align="center">

Agenda Item 10

</div>

Meeting Adjourned
The meeting adjourned at 11:55 a.m.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
048	Solicit participants with a real application to do business with Canada.	Judy Spencer, GSA	10 June 2003	13 Jan 2004 FPKIPA meeting	**Open**
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
066	Develop text for the FPKIPA Charter regarding the sunset clause for voting members of the FPKIPA who are not cross certified members of the FBCA.	Tim Polk, NIST	18 Nov 2003	13 Jan 2003 FPKIPA meeting	**Open**
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	**Open**
087	Once the CPWG approves the Department of Labor (DoL) compliance audit letter, request the FPKIPA voting members to submit their approval votes for cross certification of DoL.	Mark Lentz, Booz Allen Hamilton	13 July 2004	10 August 2004 FPKIPA meeting	**Closed, doesn't need to be an Action Item – normal processing**
090	Develop a C&A list related to NIST Standards 800-26 and 800-53.	Cheryl Jenkins, GSA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
095	Develop, obtain FPKIPA approval, and distribute a letter to cross-certification members, requesting them to send a letter to the FPKIPA to document their compliance audit history and schedule of annual audit of their cross-certified CA, in compliance with FISMA requirements.	Mark Lentz, Booz Allen Hamilton	12 Oct 2004	14 Dec 2004 FPKIPA meeting	**Closed, 01 Feb 2005**
096	Research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.	Dr. Tice DeYoung, NASA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
097	Research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.	Dr. Peter Alterman, HHS	12 Oct 2004	Jan 2005 FPKIPA meeting	**Open**
112	Update their MOA with the FBCA to reflect the new one-way certificate being issue for the period of January 2005 to January 2006.	DoD	11 Jan 2005	28 Feb 2005	**Open**
113	Prepare and route a new Letter of Authorization from the FPKIPA to the FPKI OA for this new one-way cross-certificate for the DoD PKI for the period of January 2005 to January 2006.	Mark Lentz, Booz Allen Hamilton	11 Jan 2005	31 Jan 2005	**Open**
115	Develop a FPKIPA Business Practices document.	Dr.Tice DeYoung, NASA Charles Froehlich, State (Mantech)	11 Jan 2005	31 Mar 2005	**Closed, 10 May 2005**
124	Develop a memo from the FPKIPA to the FBCA Cross-Certification members to request the maintenance of a long-term prototype CA at each of their sites.	Cheryl Jenkins, FPKI OA Director	08 Feb 2005	8 Mar 2005 FPKIPA meeting	**Open**
125	Coordinate a FBCA TWG meeting to be held in early March 2005, to discuss FBCA Directory problems identified by Treasury.	Cheryl Jenkins, FPKI OA Director	08 Feb 2005	4 Mar 2005	**Closed**
126	Determine using the Entrust CA product, how soon it will be practical to transition to the use of SHA-256.	Cheryl Jenkins, FPKI OA Director	08 Mar 2005	12 April 2005 FPKIPA meeting	**Closed**
129	If the DHS Technical Testing is approved, request an email vote for approval of DHS for Cross-Certification at the Medium assurance level.	Mark Lentz, Booz Allen Hamilton	08 Mar 2005	14 Mar 2005	**Closed, 14 March 2005**
130	Propose two dates during the 2nd week of May 2005 to choose from for scheduling a meeting for government only FPKIPA members to discuss concerns and facilitate development of a solution options for the US citizenship issue.	Tim Polk, NIST	12 Apr 2005	10 May 2005	**Open**

No.	Action Statement	POC	Start Date	Target Date	Status
131	Develop a draft position paper on this issue and report to the FPKIPA at the 14 June FPKIPA meeting.	Cheryl Jenkins, GSA Dave Hanko, DoD	12 Apr 2005	14 June 2005 FPKIPA meeting	**Open**
132	The FBCA TWG will be tasked with determining the LOE and cost necessary to post the Common Policy CA certificate in the root store cache leading email vendor products and report their findings at a future FPKIPA meeting.	Cheryl Jenkins, GSA	12 Apr 2005	14 June 2005 FPKIPA meeting	**Open**

Appendix A

FPKIPA Email Voting Record (8 Mar – 11 Apr 2005)

ORG	DHS Technical Testing Request – 9 Mar 2005 Due– 11 Mar 2005 Approval – 11 Mar 2005	Voting Member	DHS Cross-Certification (Medium) Request – 14 Mar 2005 Due – 18 Mar 2005 Approval – Mar 2005	Voting Member
Commerce	Y 03/09/05	Polk	Y 03/14/05	Polk
Defense	Y 03/11/05	Mitchell	Y 03/15/05	Hanko
Energy	Y 03/10/05	Wujcik	Y 03/16/05	Wujcik
HHS	Y 03/11/05	Alterman	Y 03/18/05	Alterman
Justice			Y 03/16/05	Deeley
State	Y 03/10/05	Cao	Y 03/14/05	Cao
Treasury			Y 03/15/05	Schminky
GSA	Y 03/10/05	Temoshok	Y 03/16/05	Temoshok
NASA	A 03/15/05	DeYoung	Y 03/17/05	DeYoung
OMB				
USDA/NFC	Y 03/09/05	Sharp	Y 03/17/05	Sharp
USPTO	N 03/10/05	Purcell		
	Result – Approved Y – 7 of 12 votes (58%) N – 1 of 12 votes (8%) A (Abstain) – 1 of 12 votes (8%) No vote cast - 3 of 12 votes (25%)		**Result – Approved** Y – 10 of 12 votes (83%)	